

**DEPARTMENT
OF
DEFENSE**

**COMPUTER SECURITY INITIATIVE:
A STATUS REPORT
AND
R&D PLAN**

MARCH 1981

**PREPARED BY THE CHAIRMAN
COMPUTER SECURITY TECHNICAL CONSORTIUM**

**INFORMATION SYSTEMS DIRECTORATE
ASSISTANT SECRETARY OF DEFENSE
COMMUNICATIONS, COMMAND, CONTROL AND INTELLIGENCE**

No Referral to OSD. On-file
release instructions apply.

DEPARTMENT

OF

DEFENSE

COMPUTER SECURITY INITIATIVE:

A STATUS REPORT

AND

R&D PLAN

MARCH 1981

Prepared by the Chairman
Computer Security Technical Consortium

Information Systems Directorate
Assistant Secretary of Defense
Communications, Command, Control, and Intelligence

TABLE OF CONTENTS

Section	Page
1 Executive Summary	1
1.1 Computer Security Initiative Activities	3
1.2 Coordination of DOD R&D Activities	6
2 Background	8
2.1 Nature of the Problem	8
2.2 Technology Development History	22
2.3 Trusted OS Fundamentals	24
2.4 System Security Vulnerabilities	29
2.5 Trusted System Environments	35
2.6 Verification Technology Overview	37
3 Computer Security Initiative Status	40
3.1 The Evaluated Products List	40
3.2 The Trusted Computing Base	46
3.3 Technology Transfer Activities	65
3.4 Trusted Computer System Evaluation	85
3.4.1 Evaluation Criteria	85
3.4.2 Evaluation Center	88
3.4.3 Evaluation Process	89
3.4.4 Summary	93
3.5 Current Evaluation Efforts	94
3.6 Status Summary	103
4 R&D Activities	104
4.1 Trusted Operating Systems	104
4.1.1 Current Research	104
4.1.2 Status of Industry Efforts	108
4.1.3 Future Directions	111
4.2 Trusted Applications	112
4.2.1 Current Research	112
4.2.2 Future Directions	118
4.3 Specification and Verification Technology	121
4.3.1 System Components	121
4.3.2 Security Properties	123
4.3.3 Current Research	124
4.3.4 R&D Plan	135
REFERENCES	142

SECTION 1

EXECUTIVE SUMMARY

Effective 1 Jan 1981 the Director of the National Security Agency was assigned the responsibility for the evaluation of computer security for the Department of Defense (figure 1-1). This function, to be called the DoD Computer Security Evaluation Center, will be responsible for advising all elements of the DoD on matters concerning the security of computer systems and in particular when the integrity of the hardware and software of a system must be relied upon. The Center will be an independent Program Management Office, separate from all other functions at NSA but drawing upon specialized skills as needed.

This report serves three purposes. The first is as a status report on the DoD Computer Security Initiative, an OSD-level effort which since mid-1978 has significantly advanced the level of understanding, both technical and managerial, of computer security and has led to the establishment of the DoD Computer Security Evaluation Center at NSA. The second purpose of this report is a summary of computer security R&D in the DoD and a projection of where future research should be directed. The third purpose of this report is as a point of departure and technical guide for the Computer Security Evaluation Center.

On 1 June 1978 ASD(C3I) formed the DoD Computer Security Technical Consortium and began the Computer Security Initiative. The goal of the Initiative is to establish widespread availability of trusted* computer systems. There are three major activities of the Initiative seeking to advance this goal: (1) coordination of DoD R&D efforts in the computer security field, (2) identification of consistent and efficient evaluation procedures for determining suitable environments for the use of trusted computer systems, and (3) encouragement of the computer industry to develop trusted systems as part of their standard product lines. This report is a summary of the activities of the Initiative since June 1978 and an

* A "trusted" computer system is one that employs sufficient hardware and software integrity measures to allow its use for simultaneously processing multiple levels of classified and/or sensitive information.